1 МАЛАЯ ТЕОРЕМА ФЕРМА (МТФ). ЧАСТЬ 1

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ ДЛЯ МНОГОЧЛЕНОВ

Рассмотрим деление с остатком для многочленов над полем $\mathbb{Z}/p\mathbb{Z}$.

Поделим многочлен

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ на многочлен

$g(x) = b_r x^r + b_{r-1} x^{r-1} + \ldots + b_1 x + b_0$ с остатком.

Считаем, что $n > r$, иначе результатом деления будет неполное частное 0 и остаток, равный самому многочлену $f(x)$.

Т.к. $\mathbb{Z}/p\mathbb{Z}$ — поле, то мы можем делить коэффициенты друг на друга.

Процесс деления продолжается, пока степень остатка не станет строго меньше, чем r. В итоге получим:

$f(x) = g(x) \cdot k(x) + h(x)$, где $\deg h < \deg g$.

Как и в наших предыдущих рассмотрениях (целых числах, гауссовых числах), на понятии деления с остатком строится вся теория, приводящая к основной теореме арифметики:

- существование НОД;
- делимость НОД на любой делитель;
- представимость НОД(a, b) в виде линейной комбинации a и b.

Никаких существенных изменений для многочленов не будет, поэтому основная **теорема арифметики верна для многочленов над полем** $\mathbb{Z}/p\mathbb{Z}$.

Вывод основной теоремы арифметики для многочленов можно найти, например, в книгах:

1. К. Айерлэнд, М.Роузен «Классическое введение в современную теорию чисел».
2. А. Савватеев «Введение в настоящую математику».

ФОРМУЛИРОВКА МАЛОЙ ТЕОРЕМЫ ФЕРМА

Вся математика устроена так. Сначала идет вводный участок, где изучается конечная арифметика, поля, факты о них. Далее идет некоторое «бутылочное горло» и за ним — новые результаты как из рога изобилия. В этом «бутылочном горле» находится необходимый результат — малая теорема Ферма, и мы уделим ее изучению достаточно продолжительное время.

Итак, мы переходим к рассмотрению конечной арифметики по простому модулю p ($p > 2$).

Система остатков $\{0, 1, 2, \ldots p - 1\}$

или по-другому $\{0, \pm 1, \pm 2, \ldots \pm \frac{p-1}{2}\}$.

Например, при $p = 13$

$\{0, 1, 2, \ldots 12\} = \{0, \pm 1, \pm 2, \ldots \pm 6\}$.

МАЛАЯ ТЕОРЕМА ФЕРМА (МТФ).

Формулировка №1

Пусть p — простое, a — любое целое.

Тогда $a^p - a \vdots p$.

Иными словами, остаток от деления числа a^p на p совпадает с остатком от деления на p самого числа a.

Формулировка №2

Пусть p — простое, a — любое целое, не делящееся на p.

Тогда $a^{p-1} - 1 \equiv 0 \bmod p$.

Эти формулировки эквиваленты, т.к. $a^p - a = a(a^{p-1} - 1)$, и делимость на p левой части означает делимость на p выражения $a^{p-1} - 1$, если a не делится на p.

УТВЕРЖДЕНИЕ О СИСТЕМЕ НЕНУЛЕВЫХ ОСТАТКОВ

Пусть p — простое, a — любое целое, не делящееся на p. Выпишем все ненулевые остатки $1, 2 \ldots p - 1$ и домножим их на a.

УТВЕРЖДЕНИЕ

$\{a, 2a, \ldots (p-1)a\}$ — тоже полная система ненулевых остатков по модулю p.

ДОКАЗАТЕЛЬСТВО

При домножении любого ненулевого остатка на ненулевой остаток a не может получиться 0, т.к. p — простое. В то же время все эти остатки различны:

$ra \equiv la \bmod p \Leftrightarrow 0 \equiv ra - la = a(r - l) \Leftrightarrow$
$r - l \equiv 0 \bmod p$ (т.к. a не делится на p) $\Leftrightarrow r \equiv l \bmod p$.

Таким образом,
$\{a, 2a, \ldots (p-1)a\}$ — просто перестановка набора различных $p - 1$ остатков. Ч.т.д.

Пример: $p = 7$, $a = 3$.
$\{a, 2a, \ldots (p-1)a\} = \{3, 6, 2, 5, 1, 4\}$.

ПЕРВОЕ ДОКАЗАТЕЛЬСТВО МТФ

Итак, $\{1, 2 \ldots p - 1\}$ — набор всех различных ненулевых остатков от деления на p. Тогда $\{a, 2a, \ldots (p-1)a\}$ — тот же набор с точностью до порядка элементов.

Мы можем приравнять произведения всех элементов:

$1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)! = a \cdot 2a \cdot \ldots \cdot (p-1)a$
$\Leftrightarrow (p-1)! \equiv a^{p-1}(p-1)! \bmod p$.
$(p-1)!$ не делится на $p \Rightarrow a^{p-1} - 1 \equiv 0 \bmod p$.

Малая теорема Ферма доказана.

Данное доказательство МТФ «в лоб» хоть и быстрое, но не дает все же полного понимания, как все работает.

Для того, чтобы рассмотреть 2-е доказательство МТФ, нам потребуется обратиться к одному из самых первых уроков и вспомнить, что такое биномиальные коэффициенты — коэффициенты в формуле бинома Ньютона.

БИНОМ НЬЮТОНА

$(a + b)^n = (a + b)(a + b) \cdot \ldots \cdot (a + b)$.

Если аккуратно перемножить все n скобок, привести подобные слагаемые и расположить их по порядку, мы получим:

$$(a + b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \ldots$$

$$\ldots + \frac{n(n-1)\ldots(n+1-k)}{k!}a^{n-k}b^k + \ldots + \frac{n(n-1)}{2!}a^2b^{n-2} + \ldots$$

$$\ldots + nab^{n-1} + b^n$$

Иными словами, $(a + b)^n = \sum_{k=0}^{n} C^k_n a^{n-k}b^k$, где

$C^k_n = \frac{n!}{k!(n-k)!} = C^{n-k}_n$ — биномиальные коэффициенты.

Почему коэффициенты именно такие?

Чтобы для любого k получить слагаемое $a^{n-k}b^k$, нам нужно выбрать в произведении n скобок $(a + b)$ те k скобок, откуда мы будем брать b, а из остальных $(n - k)$ скобок мы будем брать a. Получается $n(n - 1) \ldots (n + 1 - k)$ вариантов. При этом последовательность этих конкретных k скобок не важна, поэтому данное количество вариантов нужно разделить на количество упорядочиваний, т.е. на $k!$. Получаем формулу биномиального коэффициента для любого k.